COMMONWEALTH OF MASSACHUSETTS

DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY

Complaint of Global NAPs, Inc. Against Verizon for Denial of Issuance of Collocation Access Cards	)	**D.T.E. 03-29**

REPLY BRIEF OF VERIZON MASSACHUSETTS

As Verizon Massachusetts ("Verizon MA") demonstrates here and in its Initial Brief, Global NAPs, Inc. ("GNAPs") has no legitimate basis for seeking to eliminate Verizon MA's security practices for issuing photo identification ("ID") badges and access cards to employees and contractors of collocated carriers. Those practices apply to collocated carriers throughout the Verizon footprint and are the same as Verizon's standards for its own employees, in accordance with Federal Communications Commission ("FCC") rulings. Verizon MA's Initial Brief, at 3-5.

Maintaining the integrity of the nation's telecommunications infrastructure is critically important, now more than ever. Establishing security measures that control access to Verizon MA's central offices ("CO") is one of the most direct means of ensuring adequate protection of the network infrastructure.

Verizon MA's long-standing requirement that collocators' employees provide their Social Security numbers and place and date of birth on all new and renewal applications for access cards credentials serves legitimate security interests by enabling the Company to verify definitively the applicant's identity before allowing access to its

COs. Likewise, Verizon MA's requirement that collocated carriers certify drug testing and criminal background checks for their employees and authorized vendors is a reasonable and necessary means of better protecting the safety and security of the network, carrier equipment and personnel. The fact that GNAPs conducts *no* comparable screening of its employees and contractors only emphasizes the need to maintain Verizon MA's security practices.

This is not the time to relax or eliminate any of Verizon MA's network security measures - and GNAPs has offered no valid or compelling reason to do so. Accordingly, the Department should deny the Complaint and direct GNAPs to comply immediately with Verizon MA's security requirements.

I. ARGUMENT

A. The Employee Information that Verizon MA Requests Serves a Legitimate Security Interest and Is Not Unreasonably Intrusive, As GNAPs Erroneously Suggests.

Before issuing or renewing a non-employee ID badge and access card, Verizon MA requires personal identifying data, including the applicant's Social Security number and place and date of birth, to verify definitively the individual's identity.[1] Verizon MA's Initial Brief, at 5, 9. This is a necessary security measure - and is not "unreasonably intrusive," as GNAPs erroneously suggests.

Requesting Social Security numbers is not only standard procedure for Verizon MA, but for many other businesses and government agencies as well. Verizon MA's Initial Brief, at 9 n.10. Indeed, GNAPs admits that it obtains its employees' Social

[1] For example, Verizon MA explained in its Initial Brief that it uses Social Security number information to validate the individual's identity during the application process and when the individual experiences difficulty in accessing a premise due to access card or equipment malfunction. Verizon MA's Initial Brief, at 10 n. 12 and 13.

Security numbers, which it had provided to Verizon MA until recently. Verizon MA's Initial Brief, at 8. Verizon MA also requires its own employees to provide the same personal information required of collocators' employees. Verizon MA's Initial Brief, at 5.

Social Security number information is typically required on applications for credit cards, bank loans and accounts, and insurance policies, to name just a few of the myriad of examples. Verizon MA's Initial Brief, at 9 n.10. Contrary to GNAPs' claims, the Massachusetts Registry of Motor Vehicles also requires an individual's Social Security number on new driver's license applications and license renewals.[2] GNAPs' Initial Brief, at 9. That requirement was upheld by the Massachusetts Supreme Judicial Court. *Ostric v. Board of Appeal*, 361 Mass. 459, 462, 280 N.E.2d 692 (1972).

Plainly, the practice of requesting such personal information is not considered extraordinary or unreasonably intrusive, even where the interests to be protected are much less serious than safeguarding the telecommunications network. Further, that information is afforded strict confidential treatment within Verizon, so potential public disclosure is not a real concern. Verizon MA's Initial Brief, at 9-10.

GNAPs, however, urges the Department to accept its "trust me" approach, arguing that Verizon MA's security requirements are unwarranted for GNAPs because it is assertedly a small, family-operated company with fewer than 100 employees, most of whom are friends and family members. GNAPs' Initial Brief, at 9-10. GNAPs'

---

[2] GNAPs attempts to obfuscate the issue here. Upon request, an individual may be assigned a driver's license number other than his Social Security number. *Doe v. Registrar of Motor Vehicles*, 26 Mass. App. Ct. 415, 416 n.2, 528 N.E.2d 880 (1988). However, the Registry of Motor Vehicles still requires each individual to provide his/her Social Security number on the driver's license application and renewal. Verizon MA's Initial Brief, at 9 n.10.

approach to network security is as shockingly naïve, as it is impractical. Verizon MA does not excuse its own applicants from providing personal identifying information or undergoing drug testing or criminal background checks just because they are friends or family of existing employees. Verizon MA should not be expected to create such exemptions for GNAPs' employees.

Even if GNAPs' rationale for excusing it from the security requirements at issue made any sense (which it does not), it would not be possible to maintain a security exemption just for GNAPs. Other collocated carriers would inevitably expect and demand that the same exemptions apply equally to them. Thus, if the Department accepts GNAPs' position here, it would effectively end Verizon MA's security practices at issue here for all collocators.

Finally, GNAPs' lack of internal screening procedures for its own employees strengthens the *need* for Verizon MA to take reasonable precautions to screen those individuals who apply for access to the Company's facilities. Verizon MA's Initial Brief, at 10-11. Such employee information is used exclusively for valid, security-related purposes, and GNAPs has not proven otherwise. The Department should, therefore, deny GNAPs' Complaint.

B. Requiring Certification of Drug Testing and Criminal Background Checks for Collocated Carriers' Employees Is a Reasonable, Lawful Security Measure.

Verizon MA requires collocated carriers to certify drug test results and criminal background checks for their employees and contractors who request access to Verizon's CO. The FCC permits incumbent local exchange carriers ("ILEC") to implement such reasonable security arrangements to create a secure CO environment for itself and collocated carriers. GNAPs attempts to avoid the effect of the FCC's rulings by drawing

a distinction between security measures relating to the physical CO structure versus security measures taken to screen those individuals accessing the collocated CO facilities. GNAPs' Initial Brief, at 6. GNAPs' novel, restrictive interpretation of the FCC's rulings makes no sense.

Obviously, it is impossible for Verizon MA to safeguard the physical CO structure if it cannot reasonably control entry into that structure. In its *Advanced Services Order*,[3] the FCC provided examples of types of security devices that ILECs may utilize to protect and secure their facilities. These examples serve as guidelines, and are not intended to be all-inclusive. The fact that the FCC and Congress did not list every possible security procedure does not mean that other measures are prohibited, as GNAPs incorrectly states. GNAPs' Initial Brief, at 9, 12.

Verizon MA's first line of defense in ensuring the safety and security of its employees and its network – as well as other carriers' equipment and personnel – is screening individuals who may be a potential security risk.[4] Therefore, it makes sense - and is consistent with the letter and spirit of the FCC's decisions – that Verizon MA is permitted not only to physically fortify its COs, but also to take reasonable precautions to require certification of drug tests and criminal background checks for applicants before issuing access credentials.[5] In addition, Verizon MA imposes those same requirements

---

[3] *See Deployment of Wireline Services Offering Advanced Telecommunications Capability*, First Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 98-147, 14 FCC Rcd 4761, at ¶ 46 (March 31, 1999) ("*Advanced Services Order*").

[4] For example, an applicant who tests positively for controlled substances may unintentionally commit harmful acts in collocated facilities. Likewise, an applicant with past criminal convictions may pose a security threat, depending on the nature of the offense and other factors. Verizon MA's Initial Brief, at 5.

[5] It should be noted that GNAPs acknowledges that "wearing badges" is a reasonable security measure. GNAPs' Initial Brief, at 6. Yet, GNAPs does not explain why it neglected to renew

on its own employees for security purposes. The FCC has ruled that ILECs may impose on collocated carriers security arrangements that are as stringent as those arrangements they maintain on their premises for their own employees or authorized vendors. *Advanced Services Order*, at ¶ 47; Verizon MA's Initial Brief, at 3.

Finally, any potential privacy concerns raised by GNAPs' employees are far outweighed by the critical need to protect the telecommunications infrastructure from sabotage or other harm, especially in the post-September 11th environment. Neither federal nor state law provides an absolute right to employees to be free from drug testing. Verizon MA's Initial Brief, at 6. Likewise, Verizon MA is not legally prohibited from requiring criminal background checks relating to felony convictions for its own new employees or collocated carriers' employees in Massachusetts. Veizon MA's Initial Brief, at 7.

Verizon MA's security practices are fair and reasonable and appropriately balance the need to safeguard the network with employees' privacy interests. The Department should, therefore, deny GNAPs' Complaint.

II. CONCLUSION

GNAPs has not given the Department any basis for relaxing Verizon MA's security procedures. These procedures are patently reasonable, necessary, lawful, and applied in a nondiscriminatory manner to both Verizon MA's and collocators' employees. Accordingly, Verizon MA urges the Department to deny GNAPs' Complaint and direct GNAPs to comply with Verizon MA's security requirements, so that Verizon

---

several employees' badges prior to expiration – and how they accessed Veizon MA's COs without proper authorization, *e.g.*, by "tailgating" an authorized GNAPs' entrant, thereby bypassing any security means that would restrict access to Verizon MA's space.

MA can better protect its network and employees, as well as collocators' equipment and employees, in a time of heightened security concerns.

Respectfully submitted,

VERIZON MASSACHUSETTS

Its Attorney,

_____

Barbara Anne Sousa
185 Franklin Street, 13th Floor
Boston, Massachusetts 02110-1585
(617) 743-7331

Dated: May 23, 2003